Not-So-Smart Blockchain Contracts and Artificial Responsibility

Adam J. Kolber*

ABSTRACT

The first high-profile decentralized autonomous organization formed in 2016. Called "TheDAO," it used smart contracts on a bitcoin-style blockchain to allow strangers to come together online to vote on and invest in venture capital proposals. Newspapers raved about the $160 million it quickly raised, even though it purported to have no central human authority, including no managers, executives, or board of directors.

Technologists have grand plans for smart contracts and autonomous organizations. Rather than staying at traditional hotels with elaborate human staff, we may pay for hotel rooms using bitcoin (or another cryptocurrency) which will automatically unlock the room door. If the toilet breaks, the room itself will contract with a plumber to fix it. Similarly, a smart contract may allow us to hire a self-driving car. The car will not only drive passengers around but arrange for its own routine maintenance.

TheDAO itself, however, is now a cautionary tale. A bug in its smart contract code was exploited to drain more than $50 million in value. Some purists denounced efforts to mitigate the problem, arguing that the alleged hacker simply withdrew money in accordance with the organization's agreed-upon contractual terms in the form of computer code. Since the "code is the contract" in their minds, the alleged hacker did nothing wrong.

I defend two related claims. First, contra the purists, I argue that the code does not reflect the entirety of the parties' agreement, and so the "code is the contract" slogan does not resolve whether TheDAO exploitation should have

been mitigated. I take no position on whether mitigation was appropriate except to say that the matter depends on many considerations aside from smart contract code itself.

Second, I point to a broader danger lurking in the code-is-the-contract view. TheDAO had tremendous "artificial responsibility" in that we gave it considerable control that couldn't be easily revoked or reined in. Not-so-smart contracts in the future may prove even more dangerous: hotel guests might be locked out of their rooms, and self-driving cars might drive off bridges. I argue that unadulterated commitment to the code-is-the-contract slogan increases artificial responsibility and its associated risks.

<div align="center">TABLE OF CONTENTS</div>

<div align="center">INTRODUCTION</div>

The first robot venture capital firm opened its doors in 2016. Upon entering the large building, robots greeted eager investors who, in a matter of weeks, readily handed over $160 million to their shiny aluminum venture capitalist friends. The investors were empowered to vote on proposals to support new ventures, but all of the money was in the hands of autonomous robots. The robots were designed by humans, of course, but once created, little could be done to modify their behavior. As bad luck would have it, a bug in the robots' code enabled a thief to steal about $50 million from the firm causing the whole enterprise to fold. Though the bug became well known, the robots were simply too big and powerful for any court or police force to intervene and fix them.

You have not heard this story before because it's not entirely true. A new venture capital entity did form in 2016, but it featured online smart contracts that transferred funds according to strict rules embedded in programming code. Called "TheDAO," it was billed as the biggest crowdfunding event ever and raised about $160 million worth of

value.[1] As bad luck really did have it, a person (or team of people) exploited a loophole in those online contracts to drain what could have amounted to about $50 million in value from it.[2]

You might think that the actual story of TheDAO is less worrisome than the made-up version. After all, there were no scary robots to contend with. In many ways, though, the opposite is true. If there were robot bankers, we could have addressed TheDAO's vulnerabilities quite straightforwardly. Government officials could unplug the robots and close it down. Police could likely arrest the thief based on surveillance and other forensic evidence, and courts could ensure that everyone got as much money back as possible.

I start with the fictional version to illustrate what I call the "scary robot" illusion: namely, we worry more about the behavior of embodied machines than purely digital ones even though a machine's power and control need not be a function of its tangibility. While purely digital, TheDAO had tremendous "artificial responsibility" in the sense that it had a lot of power and control that could not be easily revoked. No single person or police force could halt it once it formed.

There were very limited options to mitigate exploitation of TheDAO.[3] Investors could potentially be made whole if enough people running the software platform that hosted TheDAO, called Ethereum, agreed to alter Ethereum's underlying code. You might have expected that path to be a no-brainer. It would save TheDAO investors a fortune, and many of them were not typical well-heeled venture capitalists with substantial assets to fall back on.[4]

Nevertheless, gathering such consensus proved no easy task. A rupture formed in the Ethereum community. Some denounced proposed

---

1. Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES (June 17, 2016), https://www.ny-times.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html [https://perma.cc/PVZ3-R2K6]; Paul Vigna, *Fund Based on Digital Currency Ethereum to Wind Down After Alleged Hack*, WALL ST. J. (June 17, 2016), https://www.wsj.com/articles/investment-fund-based-on-digital-currency-to-wind-down-after-alleged-hack-1466175033 [https://perma.cc/T57D-LG8L].

2. Popper, *supra* note 1; Vigna, *supra* note 1. The exploit made a recursive call to some computer code where the software should not have allowed it. As a result, multiple withdrawals were allowed when only one should have been permitted. Emin Gün Sirer, *Thoughts on TheDAO Hack*, HACKING, DISTRIBUTED (June 17, 2016, 09:45 AM), http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack [https://perma.cc/H2P5-SGMN].

3. Sirer, *supra* note 2 ("The DAO was not designed to have an easy 'update' function.").

4. Unlike typical venture capital investors, for example, investors in TheDAO were not asked to satisfy the income or asset requirements associated with being an "accredited investor." *See* 17 U.S.C. § 230.501.

remedies, arguing that the alleged hacker simply took advantage of contractual terms, in the form of computer code, to which all investors in TheDAO had agreed.[5] To these blockchain purists, since the computer code represents the entirety of the parties' agreement, the alleged hacker did not even do anything wrong. The taking of over $50 million from TheDAO simply exploited a feature of the contract that had gone largely unnoticed.[6] Even though some purists themselves stood to lose much of their investment in TheDAO, they were so committed to the autonomy of machines running smart contracts that they preferred to lose their money than violate what they took to be a core principle of the Ethereum platform;[7] namely that smart contract computer code *is* the contract.[8]

Thus, the downfall of TheDAO offers two big lessons about artificial responsibility: (1) Investors quickly turned over $160 million worth of value to flawed computer code that was incredibly difficult to control; and (2) once a method to rein in the machines was identified, much of the community resisted, claiming that the proposed fix violated a fundamental principle of smart contracting that the "code is the contract." (Later, I'll describe what ultimately happened to TheDAO and why the remedy proposed to fix TheDAO may not even be a realistic option in the near future.)

---

5. For some contemporaneous opinions, see, for example, the comments in these Reddit postings: Vitalik Buterin, *Personal Statement Regarding the Fork*, REDDIT (June 17, 2017), https://www.reddit.com/r/ethereum/comments/4oj7ql/personal_statement_regarding_the_fork/ [https://perma.cc/625V-NY8M]; ETH2MOON, *For All the People Who are Against the Hard Fork Let's Hear Your Alternative Solutions...*, REDDIT (July 5, 2016), https://www.reddit.com/r/ethereum/comments/4rbrdl/for_all_the_people_who_are_against_the_hard_fork [https://perma.cc/L23V-CDCZ].

6. Researchers had identified some security concerns with TheDAO before it went live, but the particular exploit had apparently never been publicly identified. *See, e.g.*, Matthew Leising, *The Ether Thief*, BLOOMBERG (June 13, 2017), https://www.bloomberg.com/features/2017-the-ether-thief [https://perma.cc/L7RZ-UGL8]; Sirer, *supra* note 2; Dino Mark, Vlad Zamfir, and Emin Gün Sirer, *A Call for a Temporary Moratorium on The DAO*, HACKING, DISTRIBUTED (May 27, 2016), http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/ [https://perma.cc/4X8G-FLBM].

7. Many purists claimed that they would rather lose value in TheDAO than alter a blockchain even if doing so was against their personal financial interests. Such claims are difficult, however, to verify.

8. The code-is-the-contract slogan is reminiscent of Larry Lessig's famous claim that "code is law," though the underlying ideas are quite distinct. *See* Larry Lessig, *Code Is Law*, HARV. MAG. (Jan. 1, 2000), https://harvardmagazine.com/2000/01/code-is-law-html [https://perma.cc/C99D-KV79] ("[C]ode . . . determines how easy it is to protect privacy, or how easy it is to censor speech. It determines whether access to information is general or whether information is zoned. . . . In a host of ways that one cannot begin to see unless one begins to understand the nature of this code, the code of cyberspace regulates.").

TheDAO shows how smart contracts and decentralized autonomous organizations ("DAOs") can wreak havoc even as purely disembodied software. Risks from these technologies may increase even more as they begin to control physical devices in the "internet of things." At a DAO hotel, you may pay for your room using a cryptocurrency, such as bitcoin,[9] which will automatically unlock your door. If the toilet breaks, the room itself will contract with a plumber to fix it. Similarly, a DAO might allow you to hire a self-driving car. After you pay, the car picks you up, drives you to your destination, perhaps arranges for its own routine maintenance, and then contracts with a new passenger.

The blockchain technology underlying bitcoin, smart contracts, and DAOs does indeed hold tremendous promise for society. Bitcoin has already smoothed transfers of value across borders.[10] Some think blockchain technology will also prove useful for managing digital identity, securities, derivatives, financial data, mortgages, land title, supply chains, auto insurance, clinical trials, and more.[11] Blockchain technologies may also offer new ways to vote and new forms of political and social organization.[12] They may increase economic efficiency and offer political and legal power to wide swaths of the population that were previously cutoff. And it's all just beginning.

On the flip side, it's easy to see how not-so-smart contracts like those underlying TheDAO can be disastrous. Given that one study

---

9. No clear convention has emerged as to the capitalization of terms like "bitcoin" and "Ethereum." Some capitalize names of software protocols but not their associated currencies, *see Does "Bitcoin" Need to Be Capitalized?*, ENG. LANGUAGE & USAGE STACK EXCHANGE (Sept. 4, 2014), https://english.stackexchange.com/questions/194653/does-bitcoin-need-to-be-capitalized [https://perma.cc/U8R7-27FU], but doing so may confuse readers. I use lower case for "bitcoin" and "ether" but capitalize "Ethereum" and "TheDAO."

10. *See* Luis Buenaventura, *There's a $500 Billion Remittance Market, and Bitcoin Startups Want in on It*, QUARTZ (Sept. 11, 2016), https://qz.com/775159/theres-a-500-billion-remittance-market-and-bitcoin-startups-want-in-on-it/ [https://perma.cc/FN84-99GY]. Recently, bitcoin transaction fees increased substantially, making cross-border payment less economical. Other cryptocurrencies have lower transaction fees, though cryptocurrencies have yet to prove that they can be both massively scalable and economically viable. Kyle Torpey, *Bitcoin is Now Useless for Micropayments, But Solutions are Coming* (Mar. 14, 2017) http://www.nasdaq.com/article/bitcoin-is-now-useless-for-micropayments-but-solutions-are-coming-cm760684 [https://perma.cc/G25J-EHV7].

11. SMART CONTRACTS ALLIANCE, SMART CONTRACTS: 12 USE CASES FOR BUSINESS & BEYOND 14-39 (2016), https://digitalchamber.org/wp-content/uploads/2018/02/Smart-Contracts-12-Use-Cases-for-Business-and-Beyond_Chamber-of-Digital-Commerce.pdf [https://perma.cc/D2XB-82NS].

12. *See generally* Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of* Lex Cryptographia, manuscript, Mar. 12, 2015, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664. [https://perma.cc/2AL7-UCJ9]; ANDREAS ANTONOPOULOS, THE INTERNET OF MONEY (2016).

flagged tens of thousands of smart contracts with possible vulnerabilities,[13] bugs like the one that plagued TheDAO are inevitable. Hotel guests could be locked out of (or maybe even inside) their rooms. Autonomous cars could drive off bridges. While physical fail-safes may protect us from some hazards, we cannot anticipate all pertinent risks. We should address these sorts of risks in advance as the steadfastness of blockchain purists may make problems harder to fix.

While legal scholars and ethicists often fret too much about new technology, there is a risk that disembodied autonomy exemplified by blockchains is less visible and therefore perceived as far less threatening than embodied autonomy. This perception will sometimes be mistaken. We must be thoughtful about the amount of responsibility we give to both embodied and disembodied machines as these technologies and the legal system co-evolve.

In Part I, I briefly describe cryptocurrencies, blockchain smart contracts, and DAOs and how they are likely to increase artificial responsibility—meaning the amount of control over important matters that we put in the hands of machines that cannot be easily vetoed or revoked by humans. This is, of course, not the sort of responsibility we ascribe to humans that warrants moral praise or blame.[14] But it is a delegation of control that is potentially dangerous and could someday turn into more robust responsibility as artificial intelligence improves.

In Part II, I argue that the code-is-the-contract slogan offered by blockchain purists is incomplete. In the case of TheDAO, the code did not reflect the entirety of the agreement among parties, and so the slogan did not resolve, for example, whether the exploitation of TheDAO should have been mitigated. I take no position on whether mitigation was appropriate except to say that it depends on many considerations aside from the software code itself.

Finally, in Part III, I offer some broad principles to guide the legal treatment of smart contracts and help address questions about which aspects of the technology, if any, require regulation. I also show how the code-is-the-contract view is not only incomplete as a matter of law and morality but is potentially dangerous, as it augments the risks inherent in artificial responsibility.

---

13. *See generally* Ivica Nikolic et al, Finding the Greedy, Prodigal, and Suicidal Contracts at Scale (Mar. 14, 2018) (unpublished manuscript) (on file with Cornell University Library system), https://arxiv.org/abs/1802.06038 [https://perma.cc/466V-WDPK].

14. *See generally* Andrew Eshleman, *Moral Responsibility*, *in* STANFORD ENCYCLOPEDIA OF PHILOSOPHY, https://plato.stanford.edu/entries/moral-responsibility [https://perma.cc/YQ87-TBLV] (Mar. 26, 2014); Adam J. Kolber, *Free Will as a Matter of Law*, *in* PHILOSOPHICAL FOUNDATIONS OF LAW AND NEUROSCIENCE, 9 (Dennis Patterson & Michael Pardo eds., 2016).

I. THE RISE OF ARTIFICIAL RESPONSIBILITY

A. *Dimensions of Machine Dangerousness*

There has been an explosion of articles in the popular press about the dangers of artificial intelligence ("AI").[15] Some fear that machines with human-like intelligence could someday develop goals at odds with our own. For example, a suitably intelligent AI that seeks to maximize the number of paper clips might, as Nick Bostrom has suggested, enslave humanity if doing so will best achieve its cold, calculated objective.[16]

But as these fears imply, what really concerns us is not so much machine *intelligence*. What we're really worried about is giving machines *control* over important matters. Control and intelligence are not the same thing. I use the expression *artificial responsibility* to refer to what scares us more directly: the ability of machines to control important matters with limited opportunities for humans to veto decisions or revoke control.

Even if an AI is a little smarter than the smartest human, it doesn't mean it can enslave us. Dominance over others isn't just a function of intelligence. We needn't be especially worried about a machine superintelligence that has no tangible control over the world unless it effectively has substantial control because of its ability to coax or manipulate us into doing its bidding. Our real concern is how easy it will be to wrest control back from machines that no longer serve our best interests and to avoid giving them control in the first place.

Self-driving cars, for example, could fall various places along a spectrum of artificial responsibility. A self-driving car that allows humans to retake control in milliseconds has limited artificial responsibility because control can be easily revoked. Though limited, it would still have substantial artificial responsibility to the extent that accidents can arise before humans can react. A self-driving car would have even more artificial responsibility if passengers had no easy opportunity to reassert control (if, say, people stop learning how to drive or if vehicles move too quickly for humans to react).

Responsibility is related to intelligence because we might be inclined to give greater control to more intelligent machines. But even un-

---

15. *See, e.g.*, Raffi Khatchadourian, *The Doomsday Invention: Will Artificial Intelligence Bring Us Utopia or Destruction?*, NEW YORKER (Nov. 23, 2015) https://www.newyorker.com/magazine/2015/11/23/doomsday-invention-artificial-intelligence-nick-bostrom [https://perma.cc/2GU3-TDZW]; Nick Bilton, *Artificial Intelligence as a Threat*, N.Y. TIMES, Nov. 5, 2014, at E2.

16. *See* NICK BOSTROM, SUPERINTELLIGENCE: PATHS, DANGERS, STRATEGIES 150-153 (2014).

intelligent machines can be dangerous when they're given a lot of responsibility. As we will see in the next section, even though blockchain technology is low on the scale of artificial intelligence (so low it is not usually thought of as artificially intelligent at all), it is nevertheless surprisingly high on the scale of artificial responsibility.

B.   Blockchains, Smart Contracts, and DAOs

1.   Blockchain Currency Such as Bitcoin

Bitcoin is a kind of digital currency invented in 2008 by a person or group of people pseudonymously known as Satoshi Nakomoto.[17] The bitcoin ecosystem enables users to store and transfer value, in the form of bitcoin, across a decentralized computer network.[18] When a bitcoin transaction commences, the transaction is broadcast to a network where nodes relay transactions to other nodes around the globe.[19]

Bitcoin "miners" solve cryptographic problems that require substantial computing power. The requirement to show proof of computational work helps maintain the security of the system. As a reward, miners can earn the right to package bitcoin transactions into "blocks"[20] and receive bitcoin in the process. New blocks are created about every ten minutes and are appended to prior blocks.[21] The collection of blocks form what is known as a "blockchain" which represents a record of all bitcoin transactions ever made. Anyone can see the record and inspect prior transactions to confirm their legitimacy. At the moment, the total value of all bitcoin is about $152 billion.[22]

While heady math underlies the cryptographic principles that keep bitcoin secure, most would say the network is rather unintelligent. It doesn't recognize our voices or faces, and it certainly wouldn't pass a Turing Test.[23] Nevertheless, it can accomplish quite a bit with limited human intervention. If bitcoin or a competitor coin is able to scale up properly, it could enable millions of people to easily transfer substantial value without the intervention of banks or other trusted intermediaries. Transactions that take banks days to accomplish, such as clearing

---

17. *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/CX9V-6RX7].

18. *See id.* at 1.

19. *Id.* at 3.

20. *Id.*

21. *Id.* at 4.

22. *Top 100 Cryptocurrencies by Market Capitalization,* COINMARKETCAP, https://coinmarketcap.com [https://perma.cc/Q7TJ-9D3K].

23. Graham Oppy & David Dowe, *The Turing Test*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (Feb. 8, 2016), https://plato.stanford.edu/entries/turing-test/ [https://perma.cc/6ERR-YN29].

checks, will be done with cryptocurrency in minutes or seconds. And the computing power behind bitcoin is extraordinary: running at about 30 exahashes per second,[24] the network puts mere supercomputers to shame.

Unintelligent as it may be, bitcoin still has substantial artificial responsibility because the network accomplishes the important task of transacting billions of dollars in value through a network spread across the globe with no person, bank, or government in charge of it. There are some laws that regulate bitcoin use. For example, bitcoin capital gains are taxed,[25] laws protect against theft,[26] and some financial regulations limit who can exchange bitcoin in particular ways.[27] Still, no single entity is capable of shutting it down. If one country banned bitcoin, it would trade in others. If every country banned it, it would likely survive—albeit in a weakened condition—[28] through black markets.

The familiar story behind bitcoin is that it is, to some extent, beyond control of banks and governments because it is run by *the people*. It might be just as accurate, however, to say that bitcoin is surprisingly autonomous not because it is run by the people but because it is run by itself.[29] It grows by paying bitcoin to miners who keep it running and allow it to grow. There may be nothing that can stop bitcoin, except perhaps for some more effective, more capable successor technology.

---

24. *Hash Rate*, BITCOIN, https://charts.bitcoin.com/chart/hash-rate [https://perma.cc/SUW5-RXBJ] (last visited Apr. 23, 2018).

25. INTERNAL REVENUE SERVICES, NOTICE 2014-21, 3, https://www.irs.gov/pub/irs-drop/n-14-21.pdf [https://perma.cc/M2GL-6H7X] (treating cryptocurrencies such as bitcoin as property for tax purposes). Some countries, however, have created opportunities to avoid paying cryptocurrency capital gains. Jose Felip, *Portugal: Profits with Bitcoin Do Not Pay Taxes*, BITCOINER.TODAY (Jan. 13, 2018), https://bitcoiner.today/en/portugal-profits-with-bitcoin-do-not-pay-taxes/ [https://perma.cc/7BSC-BXTL] (requiring no capital gains taxes on cryptocurrency sales unless they "constitute[] a professional or business activity of the taxpayer"); Kevin Helms, *Cryptocurrency Activities Will Be Legal and Tax Free in Belarus Starting in March*, BITCOIN (Jan. 18, 2018), https://news.bitcoin.com/cryptocurrencies-activities-legal-tax-free-belarus-starting-march [https://perma.cc/WJX3-DTPU] (offering tax-free sales to residents of its high-tech zone for five years).

26. *Cf.* Stan Higgins, *The FBI is Investigating a $1.3 Million Bitcoin Theft*, COINDESK (Oct. 6, 2016), https://www.coindesk.com/the-fbi-is-investigating-a-1-3-million-bitcoin-theft/ [https://perma.cc/E7F6-8TB6].

27. *See, e.g.,* 18 U.S.C. § 1960 (2018) (criminalizing the knowing operation of an unlicensed money transmitting business).

28. *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 476 (1996) (writing over a decade before bitcoin about how government regulation could make digital currencies less useful).

29. I_DID_LSD_ON_A_PLANE, Comment to *Bitcoin is the First Digital Form of Life*, REDDIT (Apr. 8, 2016), https://www.reddit.com/r/Bitcoin/comments/4du63o/bitcoin_is_the_first_digital_form_of_life [https://perma.cc/MBS9-TXV9].

2.   *Blockchain Smart Contracting Platforms Such as Ethereum*

Like the bitcoin network, the Ethereum network features a kind of cryptocurrency. Called ether, it trades like bitcoin with transactions recorded on the Ethereum blockchain. Ethereum blocks are created more quickly than bitcoin blocks, on the order of seconds rather than minutes, which may give Ethereum a competitive advantage. As of April 2018, the total value of all ether in existence is about $64 billion,[30] making it the second most popular cryptocurrency after bitcoin.

In addition to its role as a digital currency, the Ethereum network allows for the formation of "smart contracts."[31] Smart contacts can "automatically move digital assets according to arbitrary pre-specified rules."[32] For example, one might send ether to execute a betting contract with 2:1 odds on some upcoming athletic competition. When the competition is over, the Ethereum network determines which team won by, say, examining ESPN's website.[33] A winner would receive twice as much ether as he wagered. Since Ethereum smart contracts consist of particular computer code on a decentralized blockchain, it is easy to verify program execution. Once the smart contract is formed, it operates without further human intervention. While bitcoin allows some smart contracting,[34] Ethereum smart contracts are practically limitless in scope.

---

30. COINMARKETCAP, https://coinmarketcap.com [https://perma.cc/8GDU-LX3D] (last visited Apr. 23, 2018).

31. Programmer and legal scholar Nick Szabo is often credited with first describing smart contracts in 1997. *See* Nick Szabo, *Formalizing and Securing Relationships on Public Networks,* FIRST MONDAY (Sept. 1, 1997), http://firstmonday.org/ojs/index.php/fm/article/view/548/469 [https://perma.cc/VV3U-CVZF]. ("The general objectives [of smart contracts] are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries."); *see generally* Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO L. TECH. REV. 304 (2017).

32. VITALIK BUTERIN, A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM 1 (2013).

33. In this example, the contract is resolved using an "oracle." *See* Jules Dourlens, *Oracles: Bringing Data to the Blockchain*, ETHEREUM DEVELOPERS (Oct. 9, 2017), https://ethereumdev.io/oracles-getting-data-inside-blockchain/ ("In the context of blockchains, an oracle is an agent that finds and verifies real-world occurrences and submits this information to the blockchain to be used by smart contracts. The data could be the price of a currency, the weather at a given location, the result of a sport event or an election."). Ethereum developers are grappling with the challenges of identifying oracles that are sufficiently trustworthy and reliable to use in smart contracts.

34. Efforts have been made to expand bitcoin's smart contract functionality. *See, e.*g., Alyssa Hertig, *Inside MAST: The Little-Known Plan to Advance Bitcoin Smart Contracts*, COINDESK (Feb. 7, 2017, 2:00 PM), http://www.coindesk.com/inside-mast-little-known-plan-advance-bitcoin-smart-contracts   [https://perma.cc/8C5Y-F9CK]; Stan Higgins, *Rootstock Raises $1 Million to Bring Smart Contracts to*

In 2016, to illustrate the possibilities of smart contracting on the Ethereum blockchain, one group crafted an application that provides insurance in the event of a flight delay.[35] While the application was active, you could go online and find out how much it would cost to buy insurance for an upcoming flight. Based on data from prior delays, the application would then present users with the terms of a smart insurance contract. If you liked the terms, you could agree by submitting ether. Soon after an insured flight was scheduled to take off, the smart contract consulted public records to determine whether or not the flight was delayed and settled accordingly.

The application, which was made available to real-world users, foretold a world with far fewer human intermediaries. To "file" a flight delay insurance claim, there were no calls to make nor receipts to save. And because everything was automatic, in theory, there was no role for courts to play in enforcing such contracts. As one journalist put it, "Through an entry form, what previously required, and still, currently, requires, whole insurance departments and even skyscrapers, is turned into just 1s and 0s."[36] With no intermediaries between the insurer and the insured, insurance could be offered at a cheaper price. So there's a potentially efficient, disintermediating quality to blockchain smart contracts.

I wrote that smart contracts have little need for courts *in theory*. Reality, though, is more complicated. As we will see in Part II, smart contracts raise a host of legal and ethical issues, and people will no doubt attempt to create smart contracts that push legal boundaries. The flight delay app is a case in point. According to one of its creators:

> Before the launch, we were warned by several parties that launching an insurance [program] on the blockchain would very likely be considered illegal in most jurisdictions. We decided not to call it "insurance" but use the term "risk sharing" instead. Later we learned that avoiding terminology doesn't help much with regulatory compliance. Also, the fact that the contract does not check for tickets made it look more like gambling than insurance from a regulatory perspective.[37]

Bitcoin, COINDESK (Mar. 21, 2016, 2:02 PM), http://www.coindesk.com/smart-contract-1-million-bitcoin-rootstock [https://perma.cc/4HRP-ATAH].

35. Stephan Karpischek, *Flight Delay Dapp—Lessons Learned*, MEDIUM (Sept. 30, 2016), https://medium.com/the-future-requires-more/flight-delay-dapp-lessons-learned-a59e4e39a8d1 [https://perma.cc/PS2B-DVUM].

36. Andrew Quentson, *Blockchain to Disrupt Air Travel and Insurance with FlightDelay*, CRYPTOCOINSNEWS (Dec. 9, 2016, 9:11 PM), https://www.crypto-coinsnews.com/blockchain-disrupt-air-travel-insurance-flightdelay [https://perma.cc/LPY8-GV5S].

37. Karpischek, *supra* note 35.

These concerns apparently didn't stop the app's creators, perhaps because they viewed the app as a small-potatoes demonstration of smart contracting rather than a full-fledged commercial enterprise. Just a few months ago, however, a multinational insurance company announced that it is testing what sounds like a very similar flight delay insurance program on the Ethereum blockchain.[38] So it may just be a matter of time before more massive and complicated smart contracting arrangements form.

As with bitcoin, Ethereum can be understood as a network that owns itself and pays people ether to keep the network healthy and incentivize growth. Similarly, the software used to run bitcoin and Ethereum is "open source." Anyone can inspect the code and propose improvements. If those proposals are widely supported, they are incorporated into the software used to run the network. This gives Ethereum an interesting feature: smart contracts could be created to pay people to improve Ethereum. The Ethereum platform could facilitate its own evolution in a virtuous cycle that gives it more control and leads to perpetually greater artificial responsibility.

3.   *Distributed Autonomous Organizations Such as TheDAO*

Smart contacts can be combined to form a kind of organization. One contract could govern membership, another how members vote on projects, and still others on how funds are distributed, membership is terminated, and so on. In this way, we can create an entire collective that, after creation, has no human being at the helm. Such smart contracting arrangements have been called "decentralized autonomous organizations" or DAOs.

The first well-known DAO, as noted in the introduction, was called "TheDAO." The name is confusing because "DAO" is a generic name for any decentralized autonomous organization, but "TheDAO" is the name of the particular DAO at issue in this article. (Along with many others, I spell TheDAO as one word to make this clearer. We would face similar naming confusion if the first well-known corporation called itself "The Corporation.")

TheDAO accepted ether in exchange for "DAO tokens" that represented an ownership stake in TheDAO. (It would be more precise to call these "TheDAO tokens," but everyone seems to call them DAO tokens.) These tokens gave people ownership interests in TheDAO, along with proportional voting rights. A webpage for TheDAO contained terms

---

38. *AXA Goes Blockchain With Fizzy*, THE AXA GROUP (Sept. 13, 2017), https://group.axa.com/en/newsroom/news/axa-goes-blockchain-with-fizzy [https://perma.cc/YP94-PYKE].

and conditions stating that "This document does not constitute a Prospectus of any sort, is not a solicitation for investment and does not pertain in any way to an offering of securities in any jurisdiction."[39] But roughly a year after its demise, the Securities and Exchange Commission ("SEC") released a report finding that DAO tokens were, in fact, securities.[40]

TheDAO was supposed to be "[a] flexible decentralized autonomous organization leveraging the wisdom of the crowds to benefit"[41] DAO token holders, but it was not entirely autonomous. TheDAO used a small number of human "curators" to support the governance of TheDAO. For example, curators were supposed to confirm the identity of those submitting project proposals.[42] Given the short life of TheDAO, however, the precise role and potential liability of curators were never clearly defined.[43] While some claimed curators would engage in rather mechanical tasks with no significant control over TheDAO, the SEC viewed the role of curators as rather substantial.[44] To be sure, the presence of curators made TheDAO less autonomous than future decentralized autonomous organizations may be.

---

39. *Explanation of Terms and Disclaimer,* DAOHUB (July 4, 2016), daohub.org/explainer.html [https://web.archive.org/web/20160704190119/https://daohub.org/explainer.html].

40.   Press Release, U.S. Sec. and Exch. Comm'n, SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities, SEC (July 25, 2017), https://www.sec.gov/news/press-release/2017-131 [https://perma.cc/FK84-DDW9] ("In light of the facts and circumstances, the agency has decided not to bring charges in this instance, or make findings of violations in the Report, but rather to caution the industry and market participants: the federal securities laws apply to those who offer and sell securities in the United States, regardless whether the issuing entity is a traditional company or a decentralized autonomous organization, regardless whether those securities are purchased using U.S. dollars or virtual currencies, and regardless whether they are distributed in certificated form or through distributed ledger technology.").

41. DAOHUB (July 4, 2016), https://daohub.org [https://web.archive.org/web/20160704185955/https://daohub.org/].

42.   Stephen Tual, *On DAO Contractors and Curators,* SLOCK.IT BLOG (Apr. 9, 2016), https://blog.slock.it/on-contractors-and-curators-2fb9238b2553 [https://perma.cc/JA87-377D].

43. *See, e.g.,* Andrew Quentson, *Are The DAO Curators Masters or Janitors?,* COINTELEGRAPH, (June 12, 2016), https://cointelegraph.com/news/are-the-dao-curators-masters-or-janitors [https://perma.cc/5EXF-FE5R]; Alexis Roussel, *The DAO, The Curators: Evaluating and Mitigating the Legal Risks,* BITY BLOG (May 14, 2016), https://blog.bity.com/2016/05/14/the-dao-the-curators-evaluating-and-mitigating-the-legal-risks [https://perma.cc/DZB9-N69S]; Gav Would, *Why I've Resigned as a Curator of the DAO,* MEDIUM, (May 13, 2016), https://medium.com/@gavofyork/why-ive-resigned-as-a-curator-of-the-dao-238528fbd447 [https://perma.cc/ABQ6-L8EL].

44.   Securities and Exchange Commission, Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Release No. 81207, July 25, 2017, at 7, 8.

TheDAO's creators claimed that "DAOs will be at the center of many economies going forward and intend to be at the forefront of supporting innovative and promising projects, products and services . . . ."[45] TheDAO was intended "[t]o blaze a new path in business organization for the betterment of its members, existing simultaneously nowhere and everywhere and operating solely with the steadfast iron will of unstoppable code."[46] As you can see, the "unstoppability" of TheDAO was billed as a feature rather than a bug.

Remarkably, TheDAO raised about $150 million worth of value without forming a clearly recognized legal entity. DAOs are not traditional corporations. Maybe they are partnerships, but TheDAO itself had no traditional partnership agreement. Nevertheless, TheDAO raised considerable funding despite having no clear legal status, no building, and no physical address. And given the amount of money at stake, TheDAO had extraordinary artificial responsibility. Hundreds, maybe thousands, of people were locked into a collection of smart contracts that, from one point of view, ultimately stole millions of dollars from them. No single entity could shut down the apparent theft.

While the fall of TheDAO speaks to financial risks, future DAOs will risk more than just money. Had TheDAO lived on, it would have likely supported a particular company called Slock.it (whose employees helped create TheDAO)[47] and aimed to connect smart contracts to real-world devices. For example, Slock.it's technology might someday use blockchain smart contracts to control door locks, automobile ignitions, and medical devices. Thus, purely digital smart contracts can have substantial impact on the physical world when connected to devices in the internet of things. According to Bruce Schneier, such devices have already become omnipresent:

> We no longer have things with computers embedded in them. We have computers with things attached to them. Your modern refrigerator is a computer that keeps things cold. Your oven, similarly, is a computer that makes things hot. An ATM is a computer with money inside. Your car is no longer a mechanical device with some computers inside; it's a computer with four wheels and an engine. Actually, it's a distributed system of over 100 computers with four wheels and an engine . . . . We wear computers: fitness trackers and computer-enabled medical devices—and, of course, we carry our smartphones everywhere. Our homes have smart thermostats, smart appliances, smart door locks,

---

45. DAOHUB, *supra* note 41.

46. *Id.*

47. Securities and Exchange Commission, *supra* note 44, at 1,7.

even smart light bulbs. At work, many of those same smart devices are networked together with CCTV cameras, sensors that detect customer movements, and everything else. Cities are starting to embed smart sensors in roads, streetlights, and sidewalk squares, also smart energy grids and smart transportation networks. A nuclear power plant is really just a computer that produces electricity, and—like everything else we've just listed—it's on the internet. The internet is no longer a web that we connect to. Instead, it's a computerized, networked, and interconnected world that we live in. This is the future, and what we're calling the Internet of Things.[48]

Earlier, I mentioned some ways in which a DAO might connect to the internet of things. A DAO hotel might use payment on a blockchain to lock or unlock guest room doors.[49] A DAO taxi service might connect a blockchain payment to a request for a self-driving car. And even though cryptocurrencies may someday obviate the need for brick-and-mortar banks, we can imagine a DAO bank with robot tellers that dispense cash, approve loans, and give away toasters based on blockchain events.[50]

All of this has tremendous potential. But remember that TheDAO contained a bug that threatened the loss of more than $50 million worth of value. What if, in the future, a bug causes a DAO hotel to lock its guests out of their rooms or causes self-driving cars to drive off bridges?[51] What if future DAOs use evolutionary algorithms that modify the nature of the DAO over time in ways that interact with the real world in dangerous but unforeseeable ways?[52]

---

48. Bruce Schneier, *Click Here to Kill Everyone*, N.Y. Mag. (Jan 27, 2017), http://nymag.com/selectall/2017/01/the-internet-of-things-dangerous-future-bruce-schneier.html [https://perma.cc/KB76-95CH].

49. *See* Gavin Wood, *Ethereum Enthusiasts @ RISE Barclays NYC: Web 3.0 by Example*, YouTube (Apr. 7, 2016), https://www.youtube.com/watch?v=Kbu-Xbr3fdQ [https://perma.cc/Z9EJ-YSTE].

50. Indeed, China Construction Bank has already opened what is said to be the first unmanned bank branch, relying on "facial-scanning software, a virtual reality room, a hologram machine, talking robots and touchscreens for paying utility bills and Communist Party fees, among other functions." *See* Dake Kang, *Shanghai Gets Automated Bank With VR, Robots, Face Scanning*, ABC News, https://abcnews.go.com/Technology/wireStory/shanghai-automated-bank-vr-robots-face-scanning-54654991 [https://perma.cc/94S8-46JF] (last visited May 17, 2018).

51. *Cf.* Dan Bilefsky, *Hackers Use New Tactic at Austrian Hotel: Locking the Doors*, N.Y. Times (Jan. 30, 2017), https://www.nytimes.com/2017/01/30/world/europe/hotel-austria-bitcoin-ransom.html [https://perma.cc/HV3T-PA9G] (describing a hotel made to pay a bitcoin ransom in order to enable customers to enter their rooms).

52. Wright and Filippi, *supra* note 12, at 17 n.76.

As Schneier describes the internet of things, it's a "world-sized robot": "You can think of the sensors as the eyes and ears of the internet. You can think of the actuators as the hands and feet of the internet. And you can think of the stuff in the middle as the brain. We are building an internet that senses, thinks, and acts."[53] If TheDAO had its way, some control over that world-sized robot would shift from human hands to sometimes unpredictable smart contracts.

True, we can build fail-safe mechanisms into many devices to reduce the likelihood of catastrophes. But it seems unlikely that we'll foresee all the possible risks. Moreover, even events such as TheDAO exploit, though lacking immediate embodied real-world effects, still threaten so much intangible value that they can have powerful tangible consequences: the sudden loss of millions of dollars could drive some to suicide, drugs, theft, and so on. Giving machines artificial responsibility over intangibles can be no less consequential than giving them artificial responsibility over real-world machines and devices.

The combination of the blockchain and the internet of things promises tremendous opportunities to promote creativity, free expression, deliberative democracy, and economic efficiency. But given the complexity of the entire apparatus, it also raises the risk that we are creating machines that will prove difficult or even impossible to rein in.

II.WHY THE CODE IS NOT THE CONTRACT

On June 17, 2016, TheDAO imploded when about $50 million worth of ether was removed from its digital coffers.[54] Whoever took the ether exploited loopholes in the smart contracts comprising TheDAO. Anyone with sufficient technical expertise to identify the bugs could have used the same process to withdraw the funds, and unlike indisputable hacking behavior, no passwords were cracked or stolen.

The exploitation of TheDAO raised many novel legal questions.[55] Most importantly, did the exploit break laws and, if so, which ones? For example, did the person or group that exploited TheDAO commit theft or fraud or violate the Computer Fraud and Abuse Act?[56] There are many additional questions outside the criminal law as well: Was TheDAO a partnership? Did token holders have fiduciary responsibili-

---

53. Schneier, *supra* note 48.

54. Popper, *supra* note 1.

55. For discussion of many more legal issues than I address, see Drew Hinkes, *A Legal Analysis of the DAO Exploit and Possible Investor Rights*, BITCOIN MAGAZINE, June 21, 2016; Stephen D. Palley, *How to Sue TheDAO Hacker*, COINDESK, (June 17, 2016), https://www.coindesk.com/sue-dao-hacker [https://perma.cc/N56P-2ZY5].

56. *See* 18 U.S.C. § 1030 (2008); Hinkes, *supra* note 55.

ties to each other? Do TheDAO programmers or curators have any liability for the exploitation of DAO tokens?[57] Which courts around the globe have jurisdiction over which of these issues?

Is it possible that, in some crypto-jiujitsu manner, efforts to nullify the exploit would actually violate rights of the *exploiter*?[58] While it hasn't been verified as genuine, an open letter was published that purported to be from a person who exploited TheDAO. It argued that the exploit simply exercised rights provided for under smart contracts and that efforts to undo the exploitation "would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract."[59] Rather audaciously, the letter stated: "I reserve all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my legitimate ether, and am actively working with my law firm."[60]

But among the many interesting issues raised by TheDAO, I will focus on just one. It's a question that occupied much of the Ethereum community in the weeks following the exploit: Given that there were some limited ways to mitigate the loss of funds if enough people in charge of the computing power underlying the Ethereum network agreed to it, would it be inappropriate to do so on the grounds that TheDAO's smart contract code was the contract and the code permitted the exploit?

Many vehemently opposed mitigation.[61] To appreciate why, we must understand what makes blockchains valuable in the first place. Blockchains hold the promise of reducing or eliminating the need for trusted intermediaries. Networked computers work together from a shared ledger (the blockchain) that shows all pertinent transaction information, and everyone should be able to trust that no one has tampered with the data.

---

57. Note that open source software licenses often contain liability disclaimers. *See* Choose an open source license, *MIT License* (Jan. 31, 2018), https://choosealicense.com/licenses/mit [https://perma.cc/7J66-AZS3].

58. *See* Hinkes, *supra* note 55.

59. A Guest, *An Open Letter*, Pastebin (June 18, 2016, 5:21 AM), https://pastebin.com/CcGUBgDG [https://perma.cc/UZT7-BAER].

60. *Id.* The odd phrase, "illegitimate theft," suggests, perhaps unsurprisingly, that the author believes there is such a thing as legitimate theft.

61. *See, e.g.,* logical, Comment, Reddit (July 5, 2016), https://www.reddit.com/r/Ethereum/comments/4rbrdl/for_all_the_people_who_are_against_the_hard_fork/d4ztnr6 [https://perma.cc/DT29-BV7K] ("Everyone who runs the hard fork is equally complicit in betraying the rules that had been stated over and over in so many ways and so many places that modification of this kind will not happen in Ethereum. . . . Ethereum will have been turned into a blockchain with source code published as to how to make arbitrary changes en masse to it. . . . Frankly, in my view, it makes Ethereum and ether entirely worthless."); *supra* note 5.

Trust develops in a blockchain through various processes of "emergent consensus" among computers in the network. Under the "proof of work" method currently used by bitcoin and Ethereum, we expect the network to generally follow the blockchain that has the most computational resources behind it.[62] This means that any proof-of-work blockchain is vulnerable to attack by an entity with greater than 50% of the total computational resources of the entire network. Since the bitcoin and Ethereum networks are large and well-developed, attacking these networks to alter the blockchain is difficult and quite expensive, perhaps prohibitively so.

Because blockchain security is supposed to rest on emergent consensus in an immutable blockchain, there was understandably substantial resistance to anything that would "fix" the blockchain and thereby raise questions about its immutability. In the case of TheDAO exploitation, however, what some might ordinarily consider hacking, namely, amassing greater than 50% of the computational resources could also be turned into a hack-fix. If enough of the computational power supporting the Ethereum network agreed to it, the underlying software could be changed to mitigate the exploitation.

The changes to the Ethereum protocol required to mitigate the exploit were referred to as a "hard fork," because new software would lead to a new blockchain that could not be used with the software that generated the old blockchain.[63] While the newly created blockchain would likely be the one that everyone agreed to use, there was a risk that the old blockchain would not die off entirely. If not all people honored the new fork of the network and continued to add blocks to the original chain, the network could split and devalue the combined network as a whole.

As I noted, blockchain purists claimed that Ethereum should not have forked because TheDAO, rather than being hacked, was simply exploited. In a slogan, they claimed that "the code is the contract," and the person or group who exploited TheDAO simply followed the terms of

---

62. Nakamoto, *supra* note 17, at 3. ("The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains."). Some blockchains, such as Ethereum, are expected to switch to variations on this approach that build consensus without relying on massive computational power. *See, e.g.,* Alyssa Hertig, *Ethereum's Big Switch: The New Roadmap to Proof-of-Stake,* (May 16, 2017, 4:27 PM), https://www.coindesk.com/ethereums-big-switch-the-new-roadmap-to-proof-of-stake [https://perma.cc/9DP5-PUQR].

63. There is some dispute about how to precisely define a hard fork. *See* Amy Castor, *A Short Guide to Bitcoin Forks*, (Mar. 27, 2017, 2:00 PM), https://www.coindesk.com/short-guide-bitcoin-forks-explained [https://perma.cc/U2VA-P5RB]; INVESTOPEDIA, *Hard Fork*, https://www.investopedia.com/terms/h/hard-fork.asp [https://perma.cc/U8A6-5WMR].

the contract, much as one might take advantage of a loophole in a traditional contract. This purist view of how blockchains should operate highlights the risks of artificial responsibility: even when machines act in what seem to be harmful ways, some purists would prefer to allow the harm to occur rather than take the difficult steps required to revoke machine control.

After explaining the initial plausibility of the code-is-the-contract slogan, I will argue that it is false from both legal and moral perspectives. The programming code underlying TheDAO was not, by itself, the entirety of the agreement among DAO token holders. Those running the Ethereum network were collectively empowered to undue the exploit, and I argue that they need not have felt morally obliged to refrain from undoing the exploit on the ground that undoing it would upset clear contractual commitments of those using the Ethereum blockchain. None of this means that forking Ethereum was the right solution; it simply means that the code-is-the-contract slogan, by itself, fails to settle the matter.

A. *The Claim that the Code is the Contract*

I will mention two of the biggest reasons people supported the code-is-the-contract view in the context of TheDAO exploit. The first is that people investing in TheDAO likely realized that smart contracts would be understood quite literally with little role for human interpretation. Much of the impetus for creating smart contracts comes from their ability to execute without human intervention. As noted, TheDAO was based on the Ethereum platform, and when you visit Ethereum's main website, one of the first things you see is large text stating that Ethereum enables people to "[b]uild unstoppable applications."[64] In just slightly smaller text, it says that "Ethereum is a *decentralized platform that runs smart contracts*: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference."[65] So as a useful starting point, sophisticated DAO token holders should have known that the code would be taken very seriously and that human intervention is ordinarily off the table.

Second, most DAO token holders likely received more specific warnings that code in TheDAO would be mechanistically interpreted by computers. They likely bought tokens from a website called "dao-hub.org," where purchasers were warned about the hyperliteral nature of the smart contracts they were participating in. For example, a

---

64. ETHEREUM   FOUNDATION,   https://www.ethereum.org [https://perma.cc/RDH9-TLBD] (last visited Jan. 23, 2018). As noted earlier, TheDAO made similar claims of "unstoppability."

65. *Id.*

webpage called "TERMS: EXPLANATION OF TERMS AND DISCLAIMER" stated:

> The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum block-chain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all terms of The DAO Creation.[66]

Another part stated, "By Creating DAO tokens through interaction with The DAO's smart contract code, you expressly agree to all of the terms and conditions set forth in that code. If you do not understand or do not agree to those terms, you should not Create DAO tokens."[67] Still another provision stated, "The DAO's smart contract code governs the Creation of DAO tokens and supercede [sic] any public statements about The DAO's Creation made by third parties or individuals associated with The DAO, past, present and future."[68] Reasonable readers presented with this information should have realized that they were signing on to a process heavily dependent on the mechanistic interpretation of program code. (There were also secondary markets where one could purchase DAO tokens without these disclaimers,[69] but those sophisticated enough to know about these markets may have also known where to find details about the terms meant to govern DAO tokens.)

So, at least at first glance, it's easy to see why many were swayed by the code-is-the-contract slogan. Advocates claimed that TheDAO's

---

66. WAYBACK MACHINE, https://web.archive.org/web/20160523211441/https://daohub.org/explainer.html (imaged on May 23, 2016, 21:14:41). TheDAO's explanatory materials wrote "The DAO" as two words.

67. *Id.*

68*. Id.*

69. Shapeshift provided what may have been the most well-known secondary market for the purchase of DAO tokens. *See, e.g.,* SHAPESHIFT, https://www.shapeshift.io [https://perma.cc/XAR2-FZF5].

smart contract code described the entirety of the agreement made by those who joined it, so that whoever exploited TheDAO didn't *steal* tokens. He (or she or they) simply followed a contractual provision that enabled the taking of those tokens, something any of us with sufficient technical know-how could have done. TheDAO exploit may have been unexpected, but if the code is the contract, then the agreement permitted the exploitation. According to code-is-the contract advocates, nullifying the exploit would actually violate the terms that DAO token holders agreed to.

Importantly, only DAO token holders were parties to the relevant smart contracts, while a fork to mitigate the exploit required action by those running the Ethereum platform. Though many running Ethereum never assented to TheDAO's smart contracts, they may nevertheless have felt a moral obligation to right a wrong if one happened on their platform. The code-is-the-contract advocates argued that such compunction was unnecessary because there was no wrong: no rights of DAO token holders were violated by the exploiter. From their perspective, there was no obligation to fork Ethereum whatsoever, a view that many found and continue to find persuasive.

B.   Why the Code-is-the-Contract Slogan Needn't Preclude a Hard Fork

Notwithstanding the initial plausibility of the code-is-the-contract slogan, there are good reasons to believe that the exploiter violated the rights of DAO token holders such that those running Ethereum were not morally obliged to refuse to fork. Indeed, some might believe they were morally *obliged to* fork. Here are five reasons why TheDAO code should not be viewed as the entirety of a contract that would morally prohibit those running Ethereum from mitigating the exploit:

1.   Code Cannot Literally Be a Contract

First, no physical representation of an agreement can ever entirely represent the agreement. Though we informally speak of contracts as pieces of paper or text on a screen, contracts are intangible. They are enforceable agreements.[70] An agreement is not identical, however, to whatever words or other media are used to make the agreement.[71]

---

70. Not surprisingly, a "contract" has been defined in a variety of ways, including as "an agreement to do, or refrain from doing, a particular thing, upon a sufficient consideration;" "an agreement, obligation, or legal tie by which a party binds itself, or becomes bound, expressly or impliedly, to pay a sum of money or to perform or omit to do some certain act or thing;" and "an agreement between two or more parties that creates obligations that are legally enforceable by the contracting parties." *Contracts*, 17A AM. JUR. 2D CONTRACTS § 1, at 1.

71. I thank Laurent Sacharoff for emphasizing this point in discussion.

While we say things like, "Did you sign the contract?" we are really asking whether you assented to a contract whose terms appear on some piece of paper. Contract code can stipulate many terms of a contract, just as paper can. But neither code nor paper *are* contracts because contracts are not physical entities. So, taken literally, the code-is-the-contract claim is false.

Whether a mutually-binding agreement is even made in the first place cannot be reduced to a press of a button. To take a famous example,[72] we can imagine words such as "I do" having legally-binding significance at a marriage ceremony but only if made under appropriate circumstances. If spoken by actors in a play, for example, the words lose their legal significance. Genuine assent to a marriage requires more than just the appearance of assent, just as genuine assent to a contract requires more than just the press of a button. We cannot look merely at TheDAO's code to determine whether assent was genuine.

Similarly, no contract binds a person legally ineligible to contract. Suppose a ten-year-old activates a smart contract. The law usually allows minors to void contracts they enter.[73] So even if smart contracts sometimes form legally-binding agreements, the contract code would not constitute the entirety of the agreement because background law, including laws permitting minors to void contracts, would still govern the alleged agreement regardless of what the code said. Background law also includes securities law, and, in light of the SEC's report,[74] courts might invalidate certain contracts formed under TheDAO if they were ever formed in the first place.

Even the very language from daohub.org urging that "[t]he terms of The DAO Creation are set forth in the smart code" was not itself smart contract code. If that language bears on the agreement, then TheDAO code was not the entirety of the contract because the interpretive language preceding smart contract formation would also constitute part of the contract. On the other hand, if the interpretive language is not part of the contract, then it's not clear that DAO token holders agreed that the code would serve as the entirety of the contract.

2. *Interpretive Language Raises Doubt That Any Legal Agreement Was Intended*

Second, there actually was some interpretive language closely associated with the code itself. Programs often contain helpful explanatory material in a "readme" file. A readme file associated with TheDAO, by

---

72. J.L. AUSTIN, HOW TO DO THINGS WITH WORDS 6-11 (1962).

73. SAMUEL WILLISTON, 5 WILLISTON ON CONTRACTS § 9:5 (4th ed. 2017).

74. Securities and Exchange Commission, *supra* note 44.

its own terms, claims that TheDAO does not create a legal contract at all:

> Note: Although the word "contract" is used in The DAO's code, the term is a programming convention and is not being used as a legal term of art. The term is a programming convention, not a representation that the code is in and of itself a legally binding and enforceable contract. If you have questions about legal enforceability, consult with legal counsel.[75]

Soon thereafter, the readme file denies the creation of a contract in even firmer language: "Your use of the Software does not, in and of itself, create a legally binding contract in any jurisdiction and does not establish a lawyer-client relationship."[76] Even if the readme file does not settle the question of whether DAO token holders formed a legally-binding contract, the language at least bears on the intent of the parties. Hence, while a smart contract undoubtedly contains code, it does not undoubtedly constitute the entirety of a contractual agreement, at least not in the legal sense.

3.   Smart Contracts Are Arguably Different in Nature Than Traditional Legal Contracts

Third, we might think that the very nature of smart contracts is inconsistent with more familiar contracts recognized by law.[77] Typical contracts involve future performance by one or more parties. If I agree to pay you $1000 in one month if you paint my house by then, we each have future obligations. Alternatively, if I pay you $1000 now to paint my house within a month, then only you have a future obligation. In both cases, obligations extend into the future. Even vending machines create future obligations. If I put coins in your machine to buy a drink

---

75. *Decentralized Autonomous Organization (DAO) Framework,* GitHub (Aug. 17, 2017, 5:47 AM), https://github.com/slockit/DAO/blob/develop/README.md [https://perma.cc/5FQG-GPRK].

76. *Id.*; *cf. id.* ("The providers of this software neither warrant nor guarantee this software shall meet the requirements of any particular legal system to form a legally binding contract, nor it [sic] it their intention to directly or indirectly facilitate or encourage the unauthorized practice of law."). Some of the language in the readme file may merely seek to disclaim a contractual relationship between software users and creators, but overall, it seems to cast doubt on the legally-binding nature of smart contracts in TheDAO.

77. *See* Alexander Savelyev, Contract Law 2.0: "Smart" Contracts as the Beginning of the End of Classic Contract Law 17 (Dec. 14, 2016) (manuscript).

and it doesn't come out, you still owe me a drink. The vendor has a continuing obligation to satisfy its end of the bargain even after agreement to the contract is signaled by a coin deposit and button press.

By contrast, if I put ether into a smart contract so that your escrowed ether is automatically sent to me if my flight is delayed, then arguably neither of us has a future obligation as neither of us is expected to take (or refrain from taking) any action after the contract is formed. If smart contracts are deemed self-executing and self-enforcing, as some seem to think, then maybe they are simply inconsistent with traditional notions of contracting.[78] Were the Ethereum ecosystem to somehow crash after I entered into a flight delay insurance smart contact but before my flight is scheduled to leave, I would arguably not be entitled to demand any additional performance from my counterparty.

Interestingly, the more seriously we take the expression "the code is the contract," the less reason to think that a binding legal agreement is formed. If, for some reason, the code fails to properly execute, the slogan seems to leave us with only code to rely on for contract enforcement. In other words, if it is true that the code is the contract, then we arguably do not have a legal agreement since the agreement seems to be limited by the efficacy of the code itself.

We could certainly imagine the opposite approach. Smart contracts could be legally binding such that I'd still have a right to payment for a delayed flight were the Ethereum platform to somehow crash. Indeed, the best solution might be to allow smart contracting parties to explicitly decide whether they are creating legally-binding obligations. But TheDAO's readme files eschewed legally-binding status, and that weakens the case that the code was the contract. By not clearly opting for legally-binding status, it was arguably not the intent of parties to TheDAO to make the code a legally-binding contract.

4. Two Possible "Codes" Could Control

Fourth, and this may be the most important point, saying that the code is the contract is ambiguous as to precisely what is meant by "the code." Narrowly construed, the code referred to a particular smart contract or set of contracts in TheDAO. Blockchain purists tend to adopt a narrow view of the code to argue that the exploit simply followed the rules of particular smart contracts.

Broadly construed, however, "the code" is all the programming used to run TheDAO as well as the entire Ethereum ecosystem that hosted it.

---

78. *See* Stephen McJohn & Ian McJohn, *The Commercial Law of Bitcoin and Blockchain Transactions*, 47 No. 2 UNIFORM COMMERCIAL CODE L.J. ART. 4, § III (2017) (noting that some consider smart contracts legally unenforceable).

And part of the code underlying the Ethereum ecosystem is the archi-tecture to enable and resolve hard forks. From this perspective, hard forking is not precluded by the code. The architecture of the Ethereum ecosystem enables hard forking for whatever reason whenever there is sufficient agreement. Hard forking was just as much a part of the code— again, broadly construed—as the TheDAO exploit was.

And experienced users knew about the general possibility of hard forks, while almost no one knew about the particulars of the code that enabled TheDAO exploit. So if you agreed to follow the code in the broad sense, then you also agreed to the possibility of a hard fork. True, both TheDAO and Ethereum were marketed as "unstoppable," but that doesn't mean we must forget about hard forking in unexpected, emer-gency cases. If two children agree to play Monopoly based on the official rules, their expectations are not necessarily frustrated when one child must end the game early when called home for dinner. Even official rules can have understood, if largely unspoken, exceptions. Since it's not obvious that DAO token holders generally agreed to the purist's narrow version of "the code is the contract," it's not obvious that DAO token holders were somehow foregoing the opportunity to push for an Ethereum fork or have Ethereum forked on their behalf.[79]

5.   *Levels of Hyperliterality*

Finally, there's hyperliteral, and then there's *hyperliteral*. The more hyperliteral you would like the interpretation of a contract to be, the more clearly that needs to be spelled out. Suppose that you and I agree to give up candy during Lent. We further agree in writing that "No mat-ter what, we will never, ever, under any circumstances, eat candy during Lent." Then, a natural disaster strikes, and we are each stranded in our respective homes for weeks with candy as our only source of food. Even

---

79. The narrow- versus broad-code distinction points to another potential am-biguity in the code-is-the-contract view. Smart contracts are written in a high-level programming language, meaning that instructions to the computer must be "com-piled" into instructions that machines can readily execute. People could conceivably enter a smart contract based on their understanding of the high-level programming language, but over time, compilers or hardware could change in unexpected ways that affect execution of the smart contract. In such cases, saying that the "code is the contract" is ambiguous between the contract code as intended to run under the orig-inal ecosystem and contract code as it would in fact run under the ecosystem as it has evolved over perhaps many years. In other words, agreeing to the code does not necessarily mean agreeing to the ultimate execution of that code in changed envi-ronments. Well-written smart contracts may be able to prepare for future changes, *see, e.g. Introduction to Smart Contracts*, Solidity, https://solid-ity.readthedocs.io/en/develop/introduction-to-smart-contracts.html#a-simple-smart-contract [https://perma.cc/N6R3-DKHJ] (noting that smart contracts should specify appropriate compilers), but unforeseen issues could still arise.

if we have no opportunity to communicate with each other, our agreement gives us virtually no reason at all to avoid candy. It's not that we have extremely strong reason to eat it that overpowers the weight of our mutual promises. Rather, I suspect, our promises, as literal as they were intended to be, were not intended to apply in the highly improbable situation in which we found ourselves starving.

Similarly, as hyperliteral as the DAO token holders expected their agreement to be, many did not intend "the contract to be the code" in the event of a major exploitation of the ecosystem. It would take a super-hyperliteral agreement to overcome such expectations. For example, TheDAO creators could have included language stating "In the event that a person exploits a loophole in our code, we hereby agree that the exploitation will be deemed permissible and consistent with our group aims." That would have come closer to generating the kind of super-hyperliterality that might make a hard fork illegitimate.

C.   *"The Code is the Contract" as a Moral Claim*

In response to the five points above, blockchain purists might emphasize that the "code is the contract" view needn't solely concern legal agreements. Even if those running Ethereum didn't consider DAO smart contracts to be legally binding, purists could argue that, as a matter of justice and fairness, DAO token holders promised to treat the code as a binding agreement, and those running the Ethereum network should honor the agreements made on their network in accordance with the reasonable expectations generated by the Ethereum community itself.

But even in the moral context, the claim that the "code is the contract" is insufficient to resolve the matter at hand. From a moral perspective, it's not clear that people were clearly apprised that the code would constitute the entirety of the agreement for many of the reasons already given. Token holders might have thought: (1) the agreement was simply ambiguous as to what would happen if a serious exploit occurred (because it was insufficiently hyperliteral); (2) the readme file disclaimed any legal sense of contract such that reasonable expectations could guide fair play when interpreting the agreement; or (3) the whole ecosystem is part of "the code," broadly construed, such that hard forks constitute an expected risk (or benefit) of TheDAO. Thus, whether "the contract is the code" is meant to be a statement about law or morality, it is insufficient to make mitigation of TheDAO exploit illegitimate.

Of course, stating that the slogan is insufficient to rule out forking does not itself resolve whether TheDAO *ought* to have forked. There are many considerations at play. On the one hand, the exploit harmed a lot of people, and we don't want an earnest venture in reengineering soci-

etal institutions to crash and burn just because someone sought to enrich himself at others' expense. And even if most token holders knew they were embarking on a risky venture, there were almost certainly some who risked more than they should have and would have faced genuine hardship if the exploitation hadn't been mitigated. While investments in TheDAO came with some warnings, they did not have the same disclosures we ordinarily associate with investments in securities.[80]

On the other hand, much of the economic value of blockchains arises from their immutability. And even if the code-is-the-contract slogan overstates the matter, there is a very strong norm that blockchains should be immutable, and token holders should have realized that. Forking Ethereum risked destroying the value of the whole enterprise. Moreover, it appeared that any remaining value could split between the old kind of ether and the new kind to the disadvantage of all those holding ether (even those who never used ether to purchase DAO tokens).

Indeed, on July 20, 2016, the Ethereum network did fork into a version using the original ether currency that nullified TheDAO exploit, and a version using "ether classic" that did not.[81] Most of the market value went to the version that nullified the exploit.[82] While all those who held ether at the time of the fork held one ether *plus* one ether classic afterwards, the sum of both currencies was lower than the value of a single ether prior to the exploitation, at least until the market adjusted to the split over time. It's hard to say how much, if at all, the fork hurt Ethereum in the long run, but it is possible that it did. The exploiter, meanwhile, apparently walked away with millions of dollars worth of value in the form of ether classic.[83]

---

80. *See, e.g.*, Securities and Exchange Commission, *supra* note 44, at 10 ("The registration provisions of the Securities Act contemplate that the offer or sale of securities to the public must be accompanied by the 'full and fair disclosure' afforded by registration with the [Securities and Exchange] Commission and delivery of a statutory prospectus containing information necessary to enable prospective purchasers to make an informed investment decision."); 17 C.F.R. § 230.501 (describing the high net worth requirements to become an "accredited investor" in securities not registered with the SEC).

81. *See* Leising, *supra* note 6; Daniil Gorbatenko, *Ethereum's Hard Fork and the Dangers of Techno-Utopianism*, MEDIUM (Sept. 6, 2016), https://medium.com/@daniilgor/ethereums-hard-fork-and-the-dangers-of-techno-utopianism-e40f4558b1da [https://perma.cc/3BC4-3R83].

82. As of this writing, each ether is worth about $645, while each ether classic is worth about $20. https://coinmarketcap.com [https://perma.cc/7FDK-WPK2] (last visited Apr. 23, 2018).

83. Alyssa Hertig, *The Plot Thickens as DAO Attacker Trades Stolen Funds for Bitcoin*, COINDESK (Oct. 27, 2016, 7:57 PM), https://www.coindesk.com/dao-attack-hacker-trades-funds-bitcoin/. [https://perma.cc/DP3C-HRKC]. After considerable appreciation over the last year and a half, the 3.6 million ether classic that were taken, Leising, *supra* note 6, are worth about $73 million today. *See* COINMARKETCAP, https://coinmarketcap.com [https://perma.cc/7FDK-WPK2]

It is also possible, however, that while the exploit itself reduced the value of ether, at least for a period of time, forking may have preserved more value than not forking would have. Failing to mitigate the exploit might have caused a more general loss of respect for the Ethereum platform, at least in some circles. Vitalik Buterin, co-founder of Ethereum and its most public face, supported the fork, arguing that "[p]rinciples have to serve a social purpose."[84] While "[s]ome bitcoin users see the hard fork as in some ways violating their most fundamental values," Buterin noted, "I personally think these fundamental values, pushed to such extremes, are silly."[85]

My point is simply that many competing considerations bear on the question of whether TheDAO ought to have forked, and there were risks with any approach selected. I don't know the best way to resolve such issues in general, but I hope to have shown that the slogan, "the code is the contract," is insufficient alone to settle the debate.

Returning to our earlier theme, TheDAO illustrates just how tightly some would resist retaking control from machines. Some were so committed to the view that the code is the contract and thereby so willing to endow the Ethereum blockchain with artificial responsibility that they would deprive DAO token holders of millions of dollars' worth of their investments even though many would deem those token holders the rightful owners of the funds.

And whether we like it or not, artificial responsibility in the blockchain is growing: hard forks will likely be harder to accomplish in the future. As the Ethereum network grows and as any particular smart contract or DAO represents an ever-smaller percentage of the ecosystem, Ethereum stakeholders may grow increasingly unwilling to fork to correct errors.[86] Indeed, Buterin himself doubts that forking will even be an option in the future.[87] While TheDAO disaster largely found its *deus ex machina* in the form of a hard fork, future delegations of artificial responsibility may offer even fewer options to revoke machine control.

III. Principles Going Forward

It is too early to say how smart contracts should be understood by the law and how, if at all, they should be regulated. So far, they have received limited attention from regulators and that might be a good

---

(last visited Apr. 23, 2018).

84. *Id.*

85. Leising, *supra* note 6.

86. See text accompanying notes 104-108, *infra*.

87. Paul Vigna, *Ethereum Gets Its Hard Fork, and the 'Truth' Gets Tested*, Wall St. J. (July 20, 2016, 10:57 AM), https://blogs.wsj.com/money-beat/2016/07/20/Ethereum-gets-its-hard-fork-and-the-truth-gets-tested/ [https://perma.cc/6M9N-3GFR].

thing. It gives developers and entrepreneurs a chance to breathe while the best uses for blockchain technology are identified and implemented. So instead of offering some neat and tidy prescription, I propose consideration of a few general principles concerning the legal treatment of blockchain smart contracts.

1. Voluntary Agreements Should Generally Be Supported, Even Hyperliteral Ones

As a starting point, mutual agreements are good, all else being equal. If a party knowingly and voluntarily executes an agreement with particular consequences, the party did so believing that the agreement was likely to be beneficial. The same is true for the counterparty. Each party expects to be made better off, at least probabilistically. So it would be foolish to prohibit blockchain smart contracting in any broad-brushed way. Smart contracts create new opportunities for people to interact, while reducing the need for intermediaries and the costs of transactions.[88]

But can an agreement really be deemed knowing and voluntary when the nature of the agreement depends on computer code that most people cannot or do not understand? Even those capable of understanding TheDAO's code were unlikely to invest the time and energy required to closely study it. Doing so would have been far more demanding than reading the terms of service agreements written in English that most of us regularly ignore. Even when we are quite capable of understanding details of our agreements, most of us gloss over them anyhow.

Smart contracts may exacerbate concerns about incompletely understood agreements. But we can surely find ways of addressing these concerns. Independent entities could issue seals of approval when smart contracts are deemed bug-free or when an English (or other natural language) description of a smart contract is certified to accurately reflect the contract's programming code. Perhaps smart contracts will come branded in ways that give users confidence in those contracts. It will take time for people to get used to the hyperliteral nature of smart contracts, and those interfacing with laypeople (including lawyers and programmers) should make special efforts to avoid conflict and confusion. But such concerns do not seem so serious that they require broad-brushed prohibitions.

---

88. Smart contracts might also benefit government directly by creating new ways to regulate. For example, they might be used to automatically collect sales taxes, speeding up collection and reducing evasion. On what smart contracts might mean for law more generally, see Anthony J. Casey & Anthony Niblett, *The Death of Rules and Standards*, 92 IND. L.J. 1401 (2017); Raskin, *supra* note 31, at 333-37; Adam J. Kolber, *Will There Be a Neurolaw Revolution?*, 89 IND. L.J. 807, 841-44 (2014) (describing how new technologies may "concretize" the law).

2. Regulation, If Any, Should Consider Risks of Negative Externalities

If blockchains and smart contracts *only* implicated the interests of their users, the artificial responsibility they create would give us less to worry about. People who use the technology have hopefully weighed the risks they are likely to face and expect to benefit overall.

In the real world, of course, cryptocurrencies and smart contracts *can* have harmful effects on third parties. For example, hackers have used malicious software to block access to data storage at hospitals, police departments, and elsewhere, and only granted access again when victims have paid ransoms in bitcoin.[89] To be sure, ransomware attacks predate bitcoin, but bitcoin enables a convenient avenue of attack. So even though these hospitals and police departments are not using bitcoin themselves, they have suffered from the availability of the technology.

More generally, the energy consumed by the bitcoin network takes a toll on the environment. One estimate from mid-2015 claimed that a single bitcoin transaction consumed enough energy to heat 1.57 American homes for a day.[90] Demand has only increased since then:

> The computer power needed to create [one bitcoin] consumes at least as much electricity as the average American household burns through in two years, according to figures from Morgan Stanley and Alex de Vries, an economist who tracks energy use in the industry. The total network of computers plugged into the Bitcoin network consumes as much energy each day as some medium-size countries—which country depends on whose estimates you believe.[91]

It seems doubtful that all and only those using bitcoin are bearing the technology's environmental costs. So while a scaled-up bitcoin may

---

89. *See* Chris Francescani, *Ransomware Hackers Blackmail U.S. Police Departments*, NBC News (Apr. 26, 2016, 10:53 AM), https://www.nbcnews.com/news/us-news/ransomware-hackers-blackmail-u-s-police-departments-n561746 [https://perma.cc/QMH4-ZN54]; April Glaser, *U.S. Hospitals Have Been Hit by the Global Ransomware Attack*, Recode (June 27, 2017, 6:47 PM), https://www.recode.net/2017/6/27/15881666/global-eu-cyber-attack-us-hackers-nsa-hospitals [https://perma.cc/XNE5-VDFY].

90. Christopher Malmo, *Bitcoin Is Unsustainable*, Motherboard (June 29, 2015, 9:23 AM), https://motherboard.vice.com/en_us/article/bitcoin-is-unsustainable [https://perma.cc/6X7Z-ABCD].

91. Nathaniel Popper, *There Is Nothing Virtual About Bitcoin's Energy Appetite*, N.Y. Times, Jan. 21, 2018, at B1.

someday save energy by reducing reliance on brick-and-mortar institutions that themselves consume substantial energy,[92] current blockchain technologies at least raise questions about their environmental sustainability.

Blockchain technologies have other potential negative externalities, aside from energy use. For example, blockchains can be vandalized with illegal, abusive images.[93] Those with a copy of the blockchain would then have a copy of those illegal images on computers they own, potentially turning the knowing possession of that blockchain into a crime. (Until better solutions can be identified, hard forks may present the best way to eliminate illegal images, despite aspirations to keep blockchains immutable.)

The wide variety of imaginable smart contracts raises an equally wide variety of imaginable third-party harms. A person participating in a flight delay smart contract could try to delay a flight intentionally to collect insurance. Someone outside the U.S., for example, could call in a bomb threat on a U.S. plane, cost taxpayers a small fortune in law enforcement resources, create fear and misery for hundreds of travelers, and increase general travel fears, just to collect a modest payout.[94] Hence, the smart contract benefits of disintermediation and general efficiency must be weighed against the externalities smart contracts can create.

As for DAOs, we've already discussed one major externality: the implosion of TheDAO harmed many Ethereum investors who had no stake in TheDAO. By splitting Ethereum into two coins, investors now had ownership interests in two networks that were probably weaker than the prior network as a whole, at least at the time of the split. In addition, the exploiter of TheDAO may have short sold ether just prior to the exploit and profited by causing ether to lose value. Doing so harmed counterparties and perhaps the market for ether more generally.

---

92. *See* Elaine Ou, *No, Bitcoin Won't Boil the Oceans*, BLOOMBERG (Dec. 7, 2017, 10:01 AM), https://www.bloomberg.com/view/articles/2017-12-07/bitcoin-is-greener-than-its-critics-think [https://perma.cc/9SAL-DPGE] (arguing that cryptocurrency mining will likely become more efficient and may replace brick-and-mortar institutions that currently use enormous amounts of energy).

93. Sadly, this appears to have already occurred. Samuel Gibbs, *Child Abuse Imagery Found Within Bitcoin's Blockchain*, THE GUARDIAN, Mar. 20, 2018, https://www.theguardian.com/technology/2018/mar/20/child-abuse-imagery-bitcoin-blockchain-illegal-content.

94. Scirra_Tom, HACKER NEWS (Sept. 13, 2016), https://news.ycombinator.com/item?id=12486528 [https://perma.cc/568U-BRF7]. The creators of the app were aware of this risk and attempted to mitigate it by limiting the total amount of insurance on any single flight. Stephan Karpischek, *Flight Delay Dapp—Lessons Learned*, MEDIUM (Sept. 30, 2016), https://medium.com/the-future-requires-more/flight-delay-dapp-lessons-learned-a59e4e39a8d1 [https://perma.cc/5BKY-WSRK].

3. Regulation, If Needed, Could Consider Positive and Negative Distributional Effects

I cannot say much here about the difficult but important question of the role, if any, government should have in redistributing wealth. Many are concerned, however, about concentrations of wealth in small percentages of the population. The prospect of artificially intelligent robots has augmented these concerns. Many will lose jobs as cars and trucks drive themselves,[95] stores automate checkout and shelf restocking,[96] and fast-food restaurants are run almost entirely by robots.[97] A company that developed a prototype robot to prepare hamburgers bluntly stated: "Our device isn't meant to make employees more efficient. . . . It's meant to completely obviate them."[98]

Smart contracts may exacerbate job-loss concerns as fewer people are needed to facilitate interaction and exchange. Reduced reliance on trusted intermediaries may, however, have substantial benefits for those with less capital. For example, many poor people who send currency to loved ones across borders pay large fees to remittance companies. Bitcoin has already helped many transfer value at great distances with smaller fees.[99] Someday, cryptocurrency may regularly facilitate transactions more economically than banks, credit card companies, and other intermediaries do now.

Similarly, Uber has made a fortune connecting a network of passengers to a network of drivers by collecting fees for each transaction. Smart contracts and DAOs may someday enable passengers and drivers to connect directly without a corporate intermediary. If so, passengers

---

95. Alex Davies, *The Numbers Don't Lie: Self-Driving Cars Are Getting Good*, WIRED (Feb. 1, 2017), https://www.wired.com/2017/02/california-dmv-autonomous-car-disengagement/.

96. Josh Kosman, *Inside Amazon's Robot-Run Supermarket That Needs Just 3 Human Workers*, N.Y. POST (Feb. 5, 2017), https://nypost.com/2017/02/05/inside-amazons-robot-run-supermarket-that-needs-just-3-human-workers/ (suggesting that Amazon might average six human employees at each large grocery store); Mike Murphy, *Amazon Is Opening a Grocery Store with No Cashiers and No Checkout Lines,* QUARTZ (Dec. 5, 2016), https://qz.com/853205/amazon-amzn-launches-a-new-grocery-store-called-amazon-go-that-could-mean-the-end-of-checkout-lines-and-millions-of-cashier-jobs/ [https://perma.cc/HWD7-EGKV].

97. Melia Robinson, *This Robot-Powered Restaurant Could Put Fast Food Workers Out of a Job*, BUSINESS INSIDER (June 30, 2016), http://www.businessinsider.com/momentum-machines-is-hiring-2016-6 [https://perma.cc/GSB8-55JD].

98. *Id.* (quoting a 2012 statement by Momentum Machines cofounder Alexandros Vardakostas).

99. *But cf*. Torpey, *supra* note 10.

could save money and drivers could earn more. As I said, I take no position here as to whether or how governments should redistribute wealth, but at least in some respects, heavy-handed regulation of smart contracts *might* further entrench wealthy corporations at the expense of consumers.[100]

4.   Artificial Responsibility Can Be Dangerous (Don't Be Lulled by the Absence of Scary Robots)

Finally, while I think ethicists often overreact to threats posed by new technologies, there is a risk that we will downplay the threats of blockchain smart contracts and DAOs because they're purely digital and disembodied. Absent scary robots, we may fail to see the scope of the artificial responsibility with which we have endowed these technologies. Quite likely, that's what happened with TheDAO. Most investors likely had at least some awareness that blockchains are difficult or impossible to alter and that smart contracting errors can be costly, yet they poured money into TheDAO with inadequate assurances that the code was bug-free.

And the bug in TheDAO was not a fluky one-time occurrence. In July 2017, $32 million worth of ether was taken from electronic wallets after a flaw was identified in a version of Ethereum software known as Parity.[101] Just a few months later, in November 2017, Parity was embarrassed once again.[102] A user accidentally activated a command that, due to a bug, froze $150 million worth of ether, perhaps permanently.[103] This disaster revealed no obvious bad faith on anyone's part. Still, millions of dollars in value may be forever unusable due to computer code that cannot easily be changed. And the debate about whether to hard fork Ethereum to fix the November Parity incident continues to be waged.[104] All of this is just a small sample of many incidents in which

---

100. For an alternative perspective, see Ian Bogost, *Cryptocurrency Might be a Path to Authoritarianism*, ATLANTIC (May 30, 2017), https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543 [https://perma.cc/53MZ-4DL6].

101. Jordan Pearson, *How Coders Hacked Back to 'Rescue' $208 Million in Ethereum*, MOTHERBOARD   (July 24,   2017),   https://motherboard.vice.com/en_us/article/qvp5b3/how-ethereum-coders-hacked-back-to-rescue-dollar208-million-in-ethereum [https://perma.cc/GX7M-CJ5V].

102. Jordan Pearson, *Someone 'Accidentally' Locked Away $150M Worth of Other People's Ethereum Funds*, MOTHERBOARD (Nov. 7, 2017), https://motherboard.vice.com/en_us/article/ywbqmg/parity-multi-signature-wallet-vulnerability-300-million-hard-fork [https://perma.cc/VYZ6-A6TX].

103. *Id.*

104. *See, e.g.*, Adam Reese, *Parity Proposes Hard Fork to Unfreeze Funds*, ETHNEWS (Dec. 11,   2017),   https://www.ethnews.com/parity-proposes-hard-fork-to-unfreeze-funds [https://perma.cc/EX5B-7AGJ]; c-i-s-c-o, *I Support "Unfreezing" the Parity Multi-Sig Funds as Part of the Already Scheduled Constantinople Hardfork,* REDDIT

blockchain funds have been lost or stolen.[105] The benefits of block-chains and smart contracts can surely outweigh the risks, but developers, investors, and scholars should more carefully recognize and protect against worst-case scenarios.

As these examples suggest, at least in the near term, the greatest threat from machines might well be not their general intelligence but their incompetence.[106] Developers will hopefully learn from these experiences and institute more careful controls on cryptocurrency and smart contract code.[107] But it's a big world out there, and it's reasonable to expect that some future smart contracts and DAOs will be even more difficult to control and cause more harm than TheDAO and Parity incidents did.

In the future, blockchain smart contracts may interact with an artificially intelligent internet of things. Doing so will create new risks, as machine behavior becomes harder to predict.[108] Now that people can hack things like insulin pumps,[109] the cost of coding mistakes may be

---

(Nov. 7, 2017), https://www.reddit.com/r/ethereum/comments/7bdkt9/i_support_unfreezing_the_parity_multisig_funds_as [https://perma.cc/V8K4-65L3]. As of this writing, the community could go either way. *Three Million Eth Have Now Voted, 52% Are Against Restoring Parity's Eth*, TRUSTNODES (Apr. 23, 2018), https://www.trustnodes.com/2018/04/23/three-million-eth-now-voted-52-restoring-paritys-eth [https://perma.cc/37NY-KD3S].

105. *See, e.g.*, John Detrixhe, *Hackers Have Stolen $400 Million Worth of ICO Investments*, QUARTZ (Jan. 22 2018), https://qz.com/1185647/hackers-have-stolen-400-million-of-initial-coin-offerings-ico-investments-ey-says [https://perma.cc/F8HF-5XCF]; Kazuaki Nagata, *Cryptocurrency Exchange Coincheck Loses ¥58 Billion in Hacking Attack*, JAPAN TIMES (Jan. 27, 2018), https://www.japantimes.co.jp/news/2018/01/27/national/cryptocurrency-exchange-coincheck-loses-58-billion-hacking-attack/#.WvU0a5ch2Uk [https://perma.cc/6GJK-BDRT].

106. *See* Jennifer Langston, *A Q & A with Pedro Domingos: Author of 'The Master Algorithm,'* UW News, Sept. 17, 2015 http://www.washington.edu/news/2015/09/17/a-q-a-with-pedro-domingos-author-of-the-master-algorithm/ (quoting Pedro Domingos stating that "[p]eople worry that computers will get too smart and take over the world, but the real problem is that they're too stupid and they've already taken over the world."); *see generally* Kate Crawford & Ryan Calo, *There is a Blind Spot in AI Research*, 538 NATURE 311 (2016); Michael Byrne, *The Real Threat Is Machine Incompetence, Not Intelligence*, MOTHERBOARD (Feb. 6, 2017), https://motherboard.vice.com/en_us/article/jpdvjg/the-real-threat-is-machine-incompetence-not-intelligence [https://perma.cc/C454-47V7].

107. Sirer, *supra* note 2 ("It's clear that writing a robust, secure smart contract requires extreme amounts of diligence. It's more similar to writing code for a nuclear power reactor . . . than to writing loose web code.").

108. Blockchains may, however, reduce certain AI risks as they can create immutable records of the data used by AI and the actions taken based on that data. *See* Rob May, *Emerging Problems In AI, and Blockchain as a Solution*, HACKERNOON (Mar. 15, 2018), https://hackernoon.com/emerging-problems-in-ai-and-blockchain-as-a-solution-19c04883b642 [https://perma.cc/N4BK-DPJS].

109. In October 2016, Johnson & Johnson reported a vulnerability in one of its insulin pumps that could allow a person to remotely deliver unauthorized injections

more than just financial. According to computer scientist Roman Yampolskiy, "[t]he more generally intelligent and capable an entity is, the less likely it is to be predictable, controllable, or verifiable."[110] And the goals of generally intelligent machines could diverge from our own in ways that have catastrophic human costs.

Perhaps AI will someday reduce risks of smart contracting if it can interpret human intentions more flexibly than the smart contracts of today. But such machine-interpreted contracts still raise what Nick Bostrom calls the "value loading problem:" when a machine engages in complex discretionary decisionmaking, it may not accurately reflect the values we want it to have.[111] So if we ever do enlist AI to help resolve smart contract disputes, we must take care that the benefits of more flexible interpretation exceed the costs of the artificial responsibility we would thereby create.

IV. CONCLUSION

Machines follow instructions exactly as programmed. We use smart contracts to take advantage of machine hyperliterality. Nevertheless, we humans are not hyperliteral. While it's possible for us to craft hyperliteral agreements, I argue that we need to be very explicit about the fact that we're doing so. In the case of TheDAO, there is too little evidence that only the code, narrowly construed, constituted the entirety of the agreement among parties. Other factors controlled as well. To the extent an agreement was formed at all, it was sufficiently vague and open to interpretation that the Ethereum community did not have to feel compelled to permit the loss of funds.

If smart contracting continues to grow in popularity, people may need lawyers to help them understand possible smart contract consequences, and law students may have to learn fundamentals of computer coding to help fill the need. Even with reasonable precautions, though, smart contracts will sometimes contain mistakes. That's a risk we can tolerate. Mistakes are made all the time in ordinary contracts, but the benefits of traditional contracts outweigh the costs. I suspect we will reach the same conclusion about smart contracting. But we must be

---

into a patient, perhaps triggering hypoglycemia. Jim Finkle, *J&J Warns Diabetic Patients: Insulin Pump Vulnerable to Hacking*, REUTERS (Oct. 4, 2016), https://www.reuters.com/article/us-johnson-johnson-cyber-insulin-pumps-e/jj-warns-diabetic-patients-insulin-pump-vulnerable-to-hacking-idUSKCN12411L [https://perma.cc/3KNT-TC37]. While no one is known to have maliciously exploited the weakness in real life, *id.*, such dangers may increase as medical devices become more highly networked.

110. Roman V. Yampolskiy, Verifier Theory and Unverifiability 8 (Oct. 25, 2016) (unpublished manuscript), https://arxiv.org/abs/1609.00331 [https://perma.cc/SQ2X-QLDV].

111. *See* Bostrom, *supra* note 16, at 226-29.

thoughtful about delegations of artificial responsibility, especially while we have so little prior experience to guide us.